Department of Homeland Security Daily Open Source Infrastructure Report for 14 February 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports federal investigators have accused a Pennsylvania man of trying to conspire with al Qaeda to blow up major U.S. oil and gas pipelines. (See item 2)
- The Associated Press reports a company in the United Arab Emirates is poised to take over significant operations at six American ports −− New York, New Jersey, Baltimore, New Orleans, Miami, and Philadelphia −− as part of a corporate sale. (See item 12)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 13, Associated Press* — **Northeast digs out from record snowstorm.** Road crews scrambled to clear streets, and travelers stranded at airports tried to get home Monday, February 13 as the Northeast dug out from a record−breaking storm that dumped two feet or more of snow across the region. Utility workers were restoring power to tens of thousands of homes and businesses left in the dark. Winds gusting up to 50 mph knocked down power lines. The storm knocked out power across the Northeast, most severely in Maryland, where more than 150,000 customers were blacked out. More than 55,000 Baltimore Gas & Electric Company customers remained without power late Sunday, February 12, and officials said it would not likely be fully restored until Tuesday, February 14. "We're just going to have to continue to attack it," said

spokesperson Rob Gould.
Source: http://news.yahoo.com/s/ap/20060213/ap_on_re_us/snowstorm

2. *February 12, Reuters* — **Pennsylvania man accused of terrorist plot to blow up sections of the Transcontinental Pipeline, oil refineries.** Federal investigators have accused a Pennsylvania man of trying to conspire with al Qaeda to blow up major U.S. oil and gas pipelines and wreck the economy. The FBI says Michael Curtis Reynolds, 47, of Wilkes−Barre, PA, attempted to provide material aid to al Qaeda to disrupt the federal government. The allegations were disclosed in a federal transcript obtained on Friday. Reynolds has not been formally charged with terrorist offenses but has been held in a Pennsylvania jail since December 5 on the unrelated charge of possessing a hand grenade. Reynolds, who is unemployed, was drawn into an FBI sting operation in Idaho two months ago in which he meet with a purported al Qaeda operative who was really a Montana judge who monitors extremist Muslim Websites looking for potential terrorist activity. At that meeting, Reynolds expected to receive $40,000 to finance a plot to blow up sections of the Transcontinental Pipeline which carries natural gas from the U.S. Gulf Coast to New York City via Pennsylvania and New Jersey. The alleged plot also included a plan to detonate propane trucks along the Alaska Pipeline, and to blow up oil refineries in New Jersey and Wyoming.
Source: http://news.yahoo.com/s/nm/20060212/us_nm/security_pennsylva nia_dc_1

3. *February 12, Knight Ridder* — **Brazil takes a major nuclear step.** Brazil will soon fire up the region's first major uranium−enrichment plant, making it the ninth country to produce large amounts of enriched uranium, which can be used to generate nuclear energy and to make nuclear weapons. The new facility will be located in Resende, about 70 miles from Rio de Janeiro. The plant initially will produce 60 percent of the nuclear fuel used by the country's two nuclear reactors. A third reactor is in the planning stages. The government hopes to increase production to meet all of the reactors' needs and still have enough to export, Brazilian officials said. "We want to build new power plants and grow our enrichment program to be self−sufficient," said Odair Dias Goncalves, the president of Brazil's National Nuclear Energy Commission. Brazil's nuclear fuel needs −− more than 120 tons of enriched uranium a year −− don't warrant the country launching an industrial facility like Resende, especially with global supplies of the material running high, said Lawrence Scheinman, a former U.S. arms−control official. "There really isn't much justification for new enrichment facilities unless countries have a very substantial number of reactors to be serviced and don't want to depend on outside suppliers," he said.
Source: http://www.ledger−enquirer.com/mld/mercurynews/news/world/13 854156.htm?source=rss&channel=mercurynews_world

4. *February 12, Cleveland Plain Dealer (OH)* — **Small fire causes alert at Ohio nuclear plant.** Perry nuclear power plant operators declared an alert Saturday, February 9 when a fan motor for a plant ventilation system caught fire. The fire, reported at 3:06 p.m., was put out by a plant worker within three minutes using a fire extinguisher, according to a release from Akron−based FirstEnergy Corp., which operates the plant about 35 miles east of downtown Cleveland on the shores of Lake Erie. The fire was out by the time the Perry Fire Department arrived at the plant. The alert, the second−lowest of four federal emergency classifications for nuclear power plants, was declared at 3:15 p.m. and remained in effect until 5:40 p.m. What caused the fire in the plant's control building remains under investigation, spokesperson Todd Schneider said. No one

was injured. The plant continued to generate electricity at full power during the event.
Source: http://www.cleveland.com/printer/printer.ssf?/base/lake/1139737083317510.xml&coll=2

5. *February 11, Daily Sentinel (CO)* — **New safety rules slated for all U.S. coal mines.** The federal agency that oversees mine safety has drawn up new rules for coal mine emergencies, but they won't go into effect until they're published, which could be days or months. Bill York−Feirn, mine safety program manager for the Colorado Division of Minerals and Geology, said the new rules will take effect as soon as they're published in the Federal Register. York−Feirn heads up coal miner training for the state. Much of the training is required by the Mine Safety and Health Administration (MSHA), which is issuing the new rules, which are in near−final form. The agency is addressing four areas, York−Feirn said. They include requirements for more one−hour emergency breathing devices and training on how to trade off with another miner, lifelines in mine escapeways and accident notification, which call for mine operators to call the MSHA within 15 minutes of an emergency situation. This is the third time since 1978 that the MSHA has pursued an emergency temporary standard, said David G. Dye, acting assistant secretary of labor for mine safety and health. Dye said the emergency rule−making will "require the use of proven technologies and techniques to help miners evacuate quickly and safely after a mine accident."
Source: http://www.gjsentinel.com/news/content/news/stories/2006/02/11/2_12_new_mining_rules.html?cxtype=rss&cxsvc=7&cxcat=7

6. *February 09, Scotsman (UK)* — **Scotland loses bomb−grade uranium.** The Dounreay nuclear plant in the UK has lost more than half a pound of highly enriched uranium (HEU), the material used to make nuclear weapons. Official government figures show that during an internal audit of UK nuclear sites over the last year, technicians at the Caithness site could not account for some 283g of HEU. Another nuclear plant, Winfrith in Dorset, has also mislaid some HEU. The discrepancies in stores of radioactive material were revealed in the Department of Trade and Industry's (DTI) annual Nuclear Materials Balance survey. The audit has previously shown even larger gaps in the nuclear balance−sheet. The government insists that the missing material is not a cause for concern. "Whenever nuclear material is measured there is an uncertainty associated with the measurement," the DTI said. While the amount of missing uranium would not be enough for a conventional nuclear device, it could be used in a "dirty bomb", in which a conventional explosive blast is used to scatter radioactive particles. Security experts also fear that uncertainties within the nuclear system can complicate intelligence efforts against terrorist groups.
Source: http://uk.news.yahoo.com/09022006/17/dounreay−loses−bomb−gra de−uranium.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

7. *February 13, Daily Herald (TN)* — **Diesel leak forces church relocation.** Workers have pumped more than 70,000 gallons of fluid in connection with a diesel leak that prompted a Giles County, TN, church congregation to move to another building, a Tennessee Department of Environment and Conservation (TDEC) official said Thursday, February 9. Crews with First Response Inc., a Goodlettsville company that specializes in environmental cleanup, have been

at the leak's site in Giles County since early January. Dale Robinson, an underground tank specialist with TDEC, said it is impossible to say how much diesel comprised the 70,000 gallons of fluid pumped from collection trenches. The fluid consisted mostly of water, officials said. May Oil Co., which has been identified as the leak's source, reported about an 800−900 gallon shortage of diesel at its facility that occurred during the first week of January. The company drained the tank shortly after the leak was discovered January 4 at a storm sewer near Richland Creek. But Pierre Billard, director of Giles County Emergency Management, said additional fuel might have leaked during the months leading up to leak's detection. Because of the inventory process being used, the tank could have been leaking 50−100 gallons of diesel a week without being detected, he said.
Source: http://www.columbiadailyherald.com/articles/2006/02/12/top_stories/01gilescleanup.txt

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

8. *February 14, CNET News* — **FBI makes connections in data breach case.** A data security breach that has spurred at least two large banks to cancel thousands of customer debit cards appears to be connected to an older ongoing investigation in Sacramento, the FBI said Friday, February 10. Bank of America and Washington Mutual customers have received notifications from the banks that their debit cards were cancelled because of a breach. FBI Special Agent John Cauthen said the bureau and the Secret Service are investigating. Cauthen said the FBI believes the case is tied to a security breach reported in The Sacramento Bee last November, in which Golden 1 Credit Union canceled about 1,500 debit cards after being alerted to possible fraud in the Sacramento area. Someone working for that merchant is suspected of pilfering account and PIN numbers from the cards. Cauthen said the FBI and Secret Service are "working what appears to be the same debit−card case." Golden 1 said that all were used at an unidentified Sacramento business in the fall of 2005. News of a wider problem arose when The San Francisco Chronicle wrote that Bank of America had begun canceling debit cards. On Friday, the paper reported that as many as 200,000 debit−card holders could be affected.
Source: http://news.zdnet.com/2100−1009_22−6038287.html

9. *February 13, Finextra* — **Westpac bids to thwart keyloggers with onscreen keypad.** Westpac has introduced a mouse−activated keypad for users logging on to its Internet banking service. The move comes just months after Australian police busted an online crime syndicate suspected of stealing funds from Web banking customers through the use of keylogging malware. Westpac says the onscreen keypad scrambles customers IDs and passwords and renders keylogging Trojans ineffective. The bank says it is the first to introduce the technology in Australia, although similar programs have been implemented by other banks worldwide, including Citibank, Standard Bank of South Africa, and ING in Holland. Westpac's move

comes just months after police in Perth smashed a crime ring that had allegedly used keylogging software to steal "significant" sums of money from victim's bank accounts. The security and effectiveness of graphical keypads has been questioned recently following revelations that scammers are increasingly using sophisticated "screenscraper" software to neutralise these programmes. Dan Hubbard, senior director of security for Websense and an analyst with the Anti Phishing Working Group, says crimeware continues to evolve and advanced techniques are now being used to steal information: "These Trojan horses are moving beyond keylogging to now capture screenshots to obtain end−user credentials."
Source: http://finextra.com/fullstory.asp?id=14898

10. *February 11, Palm Beach Post* — **Man gets 10 years for role in ChoicePoint ID theft scandal.** The man at the center of the ChoicePoint Inc. identity theft scandal was sentenced in California Friday, February 10 for fraud. Oluwatunji Oluwatosin, the Nigerian national who helped run one of the biggest−known identity and credit card theft rings in the nation, also was ordered to pay $2 million in restitution to ChoicePoint and about $6 million to banks that suffered credit card losses because of the scandal. Investigators and prosecutors said that Oluwatosin's sentencing doesn't end the ChoicePoint case, and that they expect more arrests soon. "What is clear is that (Oluwatosin) was one of the individuals primarily responsible for obtaining access to ChoicePoint," Deputy District Attorney Jonathan Fairtlough said. But "there is still an ongoing investigation." For at least two years beginning in 2002, Oluwatosin used cellphones, fake addresses and anonymous mail drop boxes in the Los Angeles area to masquerade as a business owner and trick ChoicePoint into giving him addresses, real estate records, bank information and other details of consumers that ultimately led to millions of dollars in credit card fraud. Several other people have been arrested. Los Angeles County sheriff's Detective Duane Decker said there could be "tons" of arrests in the case.
Source: http://www.palmbeachpost.com/business/content/business/epaper/2006/02/11/a9b_choicepoint_0211.html?cxtype=rss&cxsvc=7&cx_cat=6

11. *February 10, Netcraft* — **Payment gateway StormPay battling sustained DDoS attack.** Payment gateway StormPay is recovering from a distributed denial of service attack (DDoS) that has kept its Website offline for much of the past two days. The company, which provides online payment processing for thousands of e−commerce Websites, came back online Friday, February 10, after a sustained attack that began last weekend. The DDoS on StormPay is the latest in a series of attacks on services that allow Web merchants to accept credit cards. The attacks flooded StormPay with up to six gigabits a second of data, according to Barrett Lyon, chief technology officer of Prolexic Technologies. Many web hosting companies use Stormpay to process payments for recurring services. In a December advisory, the U.S cyberdefense agency US−CERT warned of an increase in DNS amplification attacks −− also known as DNS recursion attacks.
Source: http://news.netcraft.com/archives/2006/02/10/payment_gateway_stormpay_battling_sustained_ddos_attack.html

[Return to top]

Transportation and Border Security Sector

12.

February 13, Associated Press — **Arab firm to operate six ports in U.S.** A company in the United Arab Emirates is poised to take over significant operations at six American ports as part of a corporate sale, leaving a country with ties to the September 11 hijackers with influence over a maritime industry considered vulnerable to terrorism. Dubai Ports World's purchase of London−based Peninsular and Oriental Steam Navigation Co., a $6.8 billion sale, should be approved on Monday, February 13. The British company is the fourth largest ports company in the world and its sale would affect commercial U.S. port operations in New York, New Jersey, Baltimore, New Orleans, Miami, and Philadelphia. Dubai Ports World said it won approval from a U.S. government panel that considers security risks of foreign companies buying or investing in American industry. The U.S. Committee on Foreign Investment in the United States "thoroughly reviewed the potential transaction and concluded they had no objection," the company said. Critics of the proposed purchase said a port operator complicit in smuggling or terrorism could manipulate manifests and other records to frustrate the Department of Homeland Security's already limited scrutiny of shipping containers and slip contraband past U.S. Customs inspectors.
Source: http://www.buffalonews.com/editorial/20060213/1045736.asp

13. *February 13, Associated Press* — **Turkish Airlines plane skids off JFK runway.** A Turkish Airlines flight skidded off a runway as it was landing at John F. Kennedy International Airport (JFK) on Sunday, February 12, but none of the 197 passengers were injured, said Steve Coleman, a spokesperson for the Port Authority of New York and New Jersey. The airport had been closed earlier in the day as New York was hit by a record−breaking snowstorm, and the flight was one of only a few that had been running, Coleman said. The Airbus 340 plane had been turning off the runway onto a taxiway when it skidded into a spin, said Jim Peters, of the Federal Aviation Administration. “It basically spun itself around and wound up 180 degrees from the direction in which it had been rolling,” Peters said. In a statement, Turkish Airlines said that bad weather conditions caused the airplane to skid.
Source: http://www.auburnpub.com/articles/2006/02/13/news/local_news /news09.txt

14. *February 13, Greenwich Time (CT)* — **Airport upgrades security system.** Would−be criminals and terrorists will have to contend with a new intrusion detection system that security officials say will soon be operational at New York’s Westchester County Airport. An estimated $4 million project to install the system, which will include new fences and cameras, has been under way at the airport since October 2005. Recently dug trenches extended around the inside perimeter of the airport, and earthmovers flanked a taxiway. Westchester County Airport Manager Peter Scherrer said the new system will be able to instantaneously detect security breaches of the airport's outer fence and will be constantly monitored when it goes online in June. "It's a security system that the county is putting in to meet Transportation Security Administration requirements," said Scherrer, who noted that Boston's Logan International Airport is installing a similar system. Boston's system uses thermal imaging technology, such as infrared cameras, to detect intruders based on body temperature during periods of low visibility, according to congressional testimony by Craig Coy, the airport's CEO. Westchester County Airport made headlines of its own last June, when 20−year−old Philippe Patricio landed there in a single−engine Cessna that police say he and two teenage friends stole from Danbury Municipal Airport.
Source: http://www.greenwichtime.com/news/local/scn−gt−perimeter3feb13,0,4713081.story?coll=green−news−local−headlines

15. *February 13, Department of Transportation* — **Fines against CSX Transportation.** The Federal Railroad Administration (FRA) has fined CSX Transportation (CSX) $227,000 for failure of a highway−rail grade crossing warning system to activate in advance of approaching trains in Fonda, NY. The assessed civil penalties result from a federal investigation into a February 11, 2005, fatal train−vehicle collision. FRA is assessing the statutory maximum of $27,000 for interference with the normal functioning of a grade crossing warning system that resulted in an activation failure, plus $5,000 for each of 30 counts for not reporting the activation failure within the required 15−day period. “Railroads have a duty to ensure that grade crossing active warning devices, including flashing lights and gates, work properly and to make timely reports when they fail,” Federal Railroad Administrator Joseph H. Boardman said. Improving grade crossing safety has long been a top priority for the FRA. The amount of civil penalties collected by FRA each year from railroads for violations of federal grade crossing safety regulations has tripled since 2000.
Source: http://www.dot.gov/affairs/fra0106.htm

16. *February 13, Associated Press* — **Almost 31,000 gallons of oil spills into Arthur Kill.** As many as 30,786 gallons of heavy fuel oil spilled into the Arthur Kill on Monday, February 13, during a transfer from a barge to the Chevron plant here, authorities said. The spill Monday morning stretched from the Chevron facility to Smoking Point in Staten Island, and the U.S. Coast Guard and spill response companies had set up boom boats to contain it, said Larry Cattano, the city's emergency management coordinator. The Coast Guard said Chevron had assumed responsibility for the spill and had contracted with two companies to help with the cleanup. Chevron did not immediately comment when contacted about the spill. The Coast Guard said it has halted vessel traffic from the Outer Bridge Crossing to Fresh Kills, Staten Island. The cause of the spill was being investigated by the Coast Guard.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−oilspill0213feb13,0,5625983.story?coll=ny−region−apnewjersey

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *February 13, Agricultural Research Service* — **New anti−mastitis weapon on tap for dairy cows.** Injecting a sugar into cows' udders to mobilize an immune system response may give producers an alternative to antibiotics for fighting mastitis. In trials at the Agricultural Research Service's (ARS) Bovine Functional Genomics Laboratory in Beltsville, MD, scientists Max Paape and Douglas Bannerman showed that injecting cows with the yeast sugar Poly−x reduced mastitis infection at one−twelfth the cost of antibiotics. Their patent−pending approach is based on prior studies at the lab showing that increasing milk's white blood cell count will prevent infection by mastitis−causing bacteria. When injected into non−lactating dairy cows, Poly−x

functions as a kind of bugle call that mobilizes the cells to attack mastitis pathogens. During the trials, the scientists injected 40 non−milking Holstein cows with Poly−x and 40 with antibiotics. After the cows began lactating again, the scientists checked the animals for signs of mastitis infection. Those with Poly−x had a net gain of five new infections compared to 16 for antibiotic−treated cows. Mastitis is an inflammation of cows' mammary glands that costs the U.S. dairy industry approximately two billion dollars annually in both animal and dairy−production losses. Today's control programs include diagnostic testing, herd separation, animal culling, teat dips, and antibiotic treatment.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

18. *February 12, Associated Press* — **Deer farm industry survives chronic wasting disease scare.** Four years after chronic wasting disease (CWD) was discovered in deer in Wisconsin, the state still has nearly 700 licensed deer and elk farms, but they contain thousands fewer animals than in the years before CWD was discovered. Of the 13,000 farm−raised deer or elk that have been tested for the disease, 34 tested positive for it. "It crippled our industry, but it didn't put us down entirely," said Joel Espe, president of the Wisconsin Commercial Deer and Elk Farmers Association.
CWD information: http://www.cwd−info.org/
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/politi cs/13856140.htm

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

19. *February 10, Associated Press* — **County probes radioactive leaks.** The Will, IL, State's Attorney's office has begun an investigation into why a nuclear power company did not disclose until recently a series of radioactive wastewater spills over an eight−year span. The disclosure of the investigation into the leaks at Exelon Corp.'s Braidwood Generating Plant, which occurred between 1996 and 2003, came Thursday, February 9, during a county board committee meeting discussing the spills. Chicago, IL, based Exelon could face criminal charges if it intentionally discharged tainted water at the plant about 60 miles southwest of Chicago, assistant state's attorney Phil Mock told committee members. News of the previous leaks from an underground pipeline didn't surface until late last year, when Exelon announced that an elevated level of tritium, a radioactive substance commonly found in groundwater, had been discovered at the plant's northern boundary.
Source: http://www.chicagobusiness.com/cgi−bin/news.pl?id=19497

[Return to top]

Public Health Sector

20. *February 13, Wall Street Journal* — **G−8 nations shape plan to fight diseases.** The U.S. and its wealthy allies are moving to approve a first−of−its−kind plan to encourage pharmaceuticals companies to develop vaccines for diseases that afflict countries too poor to afford them. Finance ministers from the Group of Eight major industrialized powers expect to approve a pilot project when they next get together, in Washington, DC, in April. Under an advance market commitment plan, the G−8 nations would promise to subsidize the purchase of new vaccines −− for between $800 million and $6 billion −− if pharmaceuticals companies develop ones that meet standards of efficacy and safety. Once the G−8 spends the pledged amount, the drug companies would sell the vaccine at a set discount in the developing world. The idea is to ensure that companies get a substantial, upfront, government−backed financial incentive to develop the drugs, even if they ultimately have to sell them at a low price. Advised by the World Bank and other outside experts, G−8 negotiators are working through details, including which of six Third World killers should be the test case: HIV/AIDS; malaria; tuberculosis; pneumococcus, a source of pneumonia and meningitis; rotavirus, which causes fatal diarrhea in children; or human papillomavirus, a cause of cervical cancer.
Source: http://online.wsj.com/public/article/SB113978727113671974−SRloB4dKuxEp_n_bQE5C7tsODcM_20070212.html?mod=tff_main_tff_top

21. *February 13, Agence France−Presse* — **French Indian Ocean island in grip of mosquito−borne epidemic.** An epidemic of mosquito−borne virus that causes painful, arthritis−like symptoms, is spreading relentlessly across the French Indian Ocean department of Reunion, French Health Minister Xavier Bertrand said. The toll of new infections from the disease known as chikungunya "is still running at 25,000 a week," Bertrand said, describing the outbreak as "unchanged in its severity." The president of France's Institute for Development Research (IRD), Jean−Francois Girard, said the outbreak was unprecedented. "This is the biggest epidemic (of chikungunya) ever recorded in the world," he said on Monday, February 13. Girade the remarks after a meeting of officials from the health and research ministries to beef up action against the epidemic. The meeting also brought in experts from the Pasteur Institute and the National Institute for Health and Medical Research (Inserm), as well as the IRD. The meeting decided to dispatch four scientists to Reunion on Monday, February 13, for a week−long mission to assess any risk of the virus being transmitted from a mother−to−be to her fetus and to look at ways of safely eradicating mosquitoes without harming Reunion's biodiversity. Other areas of work are in fundamental research, notably the virus' lifecycle, vaccine research and mosquito reproduction.
Source: http://news.yahoo.com/s/afp/20060213/hl_afp/francereunionhealthchikungunya_060213125705;_ylt=AjWXm_5ZYUpOp7UJPxzsAveJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

22. *February 13, Agence France−Presse* — **Bird flu alerts on three continents.** Health officials on three continents went into emergency high gear as suspected and confirmed cases of the H5N1 strain of bird flu in both humans and fowl continued to accumulate around the world. In Africa, United Nations experts joined their local counterparts on the ground in to help contain the H5N1 outbreak that has spread across poultry farms. In Indonesia, a married couple were under observation at a hospital after having developed respiratory problems and high fever after coming into contacts with chickens that died suddenly. If they test positive for H5N1, it would be the fifth known bird flu "cluster case" in Indonesia. In Europe, Italy announced that a sixth wild swan tested positive for H5N1. Health authorities in Rome called for calm, while police in

the capital reported an upsurge in calls from residents reporting dead or sick birds. "The crisis unit is now becoming an anti−panic unit with a toll−free number available for the population," Rome daily Il Messaggero reported. At the same time, officials in Brussels expected lab results Tuesday, February 14, for a dead swan found in Belgium.
Source: http://news.yahoo.com/s/afp/20060213/wl_afp/healthfluworld_0 60213134521

23. *February 13, Reuters* — **Hospitals targeted for medical equipment.** Criminal gangs in the United Kingdom are stealing expensive medical equipment from hospitals to sell on the black market to Eastern Europe and Africa, police and the National Health Service internal security service said on Monday, February 13. A hospital in York had 300,000 pounds worth of endoscopy equipment used for internal examinations taken in a recent raid, a spokesperson for North Yorkshire police said, and a hospital in Leicester had other specialist equipment stolen. The University Hospital of North Durham also had a heart scanner costing 35,000 pounds taken, police said. A spokesperson for the NHS Security Management Service said they were working closely with the police and had advised hospitals on how best to protect their equipment. "The theft of such equipment is deplorable and diverts much needed resources away from patient care," the spokesperson said. Detective Sergeant Judith Smith of North Yorkshire Police, who has been liaising with forces around the country, said she knew of 10 cases where medical equipment had been taken. "There are quite a few similarities in the cases we have seen," she said. "It seems they are organized by groups or a group of individuals who know what they are doing.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=topNews&storyID=2006−02−13T130415Z_01_L13187692_RTRUKOC_0_UK−CRIME−BRITAIN−HOSPITALS.xml&archived=False

24. *February 12, Associated Press* — **Nigeria ignores bird flu precautions.** Nigeria ignored international recommendations for stopping bird flu, keeping poultry markets open on Sunday, February 12, and letting people move their birds around most of the country unrestricted. Officials were awaiting word on whether the virus already had infected people in Africa's most populous nation. Test results were pending on two sick children near a farm where the H5N1 strain was first detected among poultry. Their families also were being tested. Tope Ajakaiye, a spokesperson for Nigeria's Agriculture Ministry, said there were no plans to close poultry markets or restrict the trade or movement of poultry as recommended by international organizations. Sub−Saharan Africa, with about 600 million of the world's poorest people, is particularly ill−suited to deal with a health crisis. With weak and impoverished governments in regions where many people keep chickens for food, experts say mass killings to help control bird flu will be hard to carry out properly. Health authorities worry the virus may have already spread undetected elsewhere in Africa. The virus has been confirmed at five farms in northern Nigeria, killing at least 100,000 birds. Nigeria has about 130 million people and 140 million poultry.
Source: http://news.yahoo.com/s/ap/20060212/ap_on_he_me/bird_flu;_ylt=Ahd7O.Gh_Dp0UjTtdRm3mpNZ24cA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

25. *February 12, Agence France−Presse* — **Tests confirm two more Indonesian bird flu deaths.** Results of tests by the World Health Organization (WHO) showed that two Indonesian women who died in hospital last week had died of bird flu, a hospital spokesperson said. A

27−year−old who died at the Julianti Saroso hospital on Friday, February 10, and a 22−year−old who died a day earlier both tested positive for the H5N1 strain of the virus. The confirmation by a WHO laboratory in Hong Kong takes Indonesia's death toll from the virus to 18. Both had already been declared positive in locally conducted tests. Meanwhile, an 11−month−old baby was admitted Saturday, February 11, to the hospital suffering bird flu symptoms. Many Indonesians live with chickens around their homes, even in urban areas, creating ideal conditions for infections to pass from the birds to humans. A WHO team warned last month that Indonesia needed to focus more on measures aimed at preventing such virus transmission and also on preparations for a possible human pandemic.
Source: http://news.yahoo.com/s/afp/20060212/hl_afp/healthfluindonesiatoll_060212070923;_ylt=ApQMwjHCXpbmaX0FE.PSSRqJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *February 13, Tampa Bay Newspapers (FL)* — **Florida promotes weather awareness.** Hazardous Weather Awareness Week is an annual statewide campaign in Florida to educate residents and visitors about a variety of weather−related dangers. This year's awareness week is February 12−18. Emergency officials have planned several activities statewide focusing on different hazards Florida residents could encounter. According to the Hurricane Herald, a publication produced by the Florida Department of Community Affairs and the Division of Emergency Management, the activities include a different hazard each day. Monday was lightening awareness day. Tuesday's focus is marine hazards and rip currents. On Wednesday, tornadoes and thunderstorms will be in the spotlight, and plans call for a statewide tornado drill. Thursday is hurricane and flooding awareness day. Friday will highlight the dangers of temperature extremes and wildfires.
Hurricane Herald publication: http://www.floridadisaster.org/kids/index2.htm
Source: http://www.tbnweekly.com/content_articles/021206_fpg−01.txt

27. *February 13, Government Accountability Office* — **GAO−06−403T: Expedited Assistance for Victims of Hurricanes Katrina and Rita: FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse (Testimony).** As a result of widespread congressional and public interest in the federal response to Hurricanes Katrina and Rita, the Government Accountability Office (GAO) conducted an audit of the Individuals and Households Program (IHP) under Comptroller General of the United States statutory authority. Hurricanes Katrina and Rita destroyed homes and displaced millions of individuals. In the wake of these natural disasters, the Federal Emergency Management Agency (FEMA) faced the challenge of providing assistance quickly and with minimal "red tape," while having sufficient controls to provide assurance that benefits were paid only to eligible individuals and

households. In response to this challenge, FEMA provided $2,000 in IHP payments to affected households via its Expedited Assistance (EA) program. These payments were made via checks, electronic fund transfers, and a small number of debit cards. GAO's testimony will provide the results to date related to whether (1) controls are in place and operating effectively to limit EA to qualified applicants, (2) indications exist of fraud and abuse in the application for and receipt of EA and other payments, and (3) controls are in place and operating effectively over debit cards to prevent duplicate EA payments and improper usage.
Highlights: http://www.gao.gov/highlights/d06403thigh.pdf
Source: http://www.gao.gov/new.items/d06403t.pdf

28. *February 13, Department of Homeland Security* — **Remarks by Department of Homeland Security Secretary Michael Chertoff at the National Emergency Management Association conference.** Department of Homeland Security Secretary Michael Chertoff announced several new measures designed to strengthen the Federal Emergency Management Agency's (FEMA) essential functions so it can more effectively respond to manmade or natural disasters, particularly during catastrophic events. These new measures are designed to match the experience and skills of FEMA employees with 21st century tools and technology −− maximizing the agency's performance regardless of disaster size or complexity. The Department of Homeland Security's fiscal year 2007 budget request also asks for increased funding to begin strengthening FEMA −− specifically a 10 percent increase in FEMA's budget over this fiscal year. This budget request also provides additional resources to upgrade FEMA's Emergency Alert System; increase FEMA's procurement staff and overall capabilities; improve capital infrastructure and information technology; and strengthen overall mitigation, response and recovery capabilities.
Remarks by Secretary Chertoff: http://www.dhs.gov/dhspublic/display?content=5414
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0856.xml

29. *February 10, Inside Bay Area (CA)* — **California governor asked to update aging disaster plans.** California Senate President Pro Tem Don Perata asked Governor Arnold Schwarzenegger Thursday, February 9, to convene an emergency preparedness council, saying six outdated plans for catastrophes such as earthquakes, radiological attacks and spills of oil or hazardous materials are up to 38 years old. Perata also said recent hearings by various agencies have exposed the need for "overarching analysis" of gaps in preparedness for natural disasters and terrorism attacks, and said he is arranging an in−depth, independent study. Schwarzenegger's aides have informally said they would look into the situation, said Perata spokesperson Alicia Dlugosh. The Senate leader said he wants a meeting of the California Emergency Council, which advises the governor on preparing for catastrophes, to "address concerns identified about the state's emergency preparedness infrastructure and our capability for responding to a major crisis." Not only are there gaps in new emergency plans and other concerns, he said, but some of the guides were written decades ago and have not been updated for 15 or more years.
Source: http://www.insidebayarea.com/ci_3494870?source=rss

30. *February 10, Government Computer News* — **DICE06 Objective: Create interoperability between DoD and civilian first responder systems.** An exercise to promote systems interoperability kicked off last week across the Department of Defense (DoD). The Defense Interoperability Communication Exercise 2006 (DICE06) started earlier last week to test

communications equipment and systems for use among DoD services and agencies and with the Department of Homeland Security and first responders, according to a release sent out by the Defense Information Systems Agency. DICE06 testing will continue through April 14 at Joint Interoperability Test Command Fort Huachuca, AZ, and other locations, including Fort Monmouth, NJ, Fort Monroe, VA, Camp Pendleton, CA, and Okinawa, Japan. DICE is the largest communications exercise that tests Defense and non−DOD communication systems, according to the release. Its goal is to create interoperability among systems that support the war on terrorism and natural disasters such as Hurricane Katrina. Exercise participants include communications personnel from each of the services, the Northern Command, the Coast Guard, Federal Emergency Management Agency and state, county and municipal first responders.
Source: http://www.gcn.com/vol1_no1/daily−updates/38235−1.html

31. *February 10, GovExec* — **Pentagon shares some lessons learned from Hurricane Katrina.** Senior Department of Defense officials on Thursday, February 9, outlined some of the critical lessons the Pentagon has learned from Hurricane Katrina that could help improve the federal government's response to future catastrophes. The officials told the Senate Homeland Security and Governmental Affairs committee that the department is still in the midst of completing a full report, but that some of the issues that need to be addressed are already evident. Paul McHale, assistant secretary of defense for homeland defense, testified along with Navy Adm. Timothy Keating, commander of U.S. Northern Command, and Army Lt. Gen. Steven Blum, chief of the National Guard Bureau. Among McHale's suggestions, the government should: Improve its ability to obtain accurate assessments of damaged areas immediately after a disaster; establish a unified command and control structure to coordinate the efforts of multiple federal agencies when they converge on an affected area; assure the ability to effectively communicate with first responders and emergency management personnel. Keating said active−duty forces lacked the ability to fully know what National Guard forces were doing throughout the relief operations. Keating also cited the need for mobile, secure communications that are "survivable and flexible" and have both voice and data capabilities.
Source: http://www.govexec.com/story_page.cfm?articleid=33378&dcn=to daysnews

[Return to top]

Information Technology and Telecommunications Sector

32. *February 13, Associated Press* — **Man threatens to attack Olympic computers.** A would−be hacker was being investigated by police Monday, February 13, after threatening to attack the internal computer network of the Turin, Italy, Olympics organizing committee. The man −− a technical consultant for the Turin Organizing Committee −− illicitly gained access to off−limits sections of the network, police officer Fabiola Silvestri said. "This consultant −− who is now a former consultant −− said in a very strong way that he could do certain things to the network," Turin Organizing Committee spokesperson Giuseppe Gattino said. "Nothing has happened and all the passwords have been disabled." In a separate case, police found that a Turin antiques dealer had acquired five Internet domains that had similar names to Olympic Websites. If accessed, the domains redirected users to the dealer's Website, which also carried Olympic logos and other copyrighted material, Silvestri said. Once he had been told that what he was doing was illegal, the dealer deleted the material and redirected users from his domains to Olympic Websites, she said.

Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/02/13/AR2006021300387.html

33. *February 10, Secunia* — **IBM Lotus Domino iNotes Client script insertion vulnerabilities.** Some vulnerabilities have been reported in Lotus Domino iNotes Client, which can be exploited by malicious people to conduct script insertion attacks. Analysis: 1) Attached files (e.g. ".html" files) are opened in the context of the site if the user clicks on it. This can be exploited to execute arbitrary JavaScript code in the context of the user's session. 2) The e−mail subject is not properly sanitized before being displayed to the user as the browser title. This can be exploited to execute arbitrary JavaScript in the context of the user's session when the user views a received e−mail. 3) It is possible to bypass certain security checks related to "javascript:" URLs by inserting "
" in the middle of the URL. This can be exploited to execute arbitrary JavaScript code in the context of the user's session. 4) The attachment filename is not properly sanitized before being displayed to the user. This can be exploited to execute arbitrary JavaScript in context of the user's session when the user views a received e−mail. Solution: Update to version 6.5.5 or 7.0.1.
Source: http://secunia.com/advisories/16340/

34. *February 10, Security IT Hub* — **Hacker indicted for hospital botnet attack.** A 20−year−old California man was indicted in Seattle Friday, February 10, on charges that he used a computer "bot" network to cause computer malfunctions at Seattle's Northwest Hospital in January of 2005. Christopher Maxwell, of Vacaville, CA, was indicted by a federal grand jury on two counts of conspiracy to cause damage to a protected computer and commit computer fraud. He is alleged to have compromised computers at a number of U.S. universities for a large botnet that generated $100,000 in payments from advertising software companies, according to a statement released by the U.S. Attorney's Office for the Western District of Washington. Maxwell is alleged to have hacked computer networks at California State University, Northridge; the University of Michigan; and University of California, Los Angeles, using high−powered computers on those networks as part of an adware distribution operation.
Source: http://security.ithub.com/article/DOJ+Indicts+Hacker+for+Hospital+Botnet+Attack/171336_1.aspx

35. *February 10, Security IT Hub* — **EFF: Don't use Google Desktop.** A high−profile privacy watchdog group has a terse warning for business and consumer users: Do not use the new version of Google Desktop. The nonprofit Electronic Frontier Foundation (EFF) said a new feature added to Google Desktop on Thursday, February 9, is a serious privacy and security risk because of the way a user's data is stored on Google's servers. The new "Share Across Computers" feature stores Web browsing history, Microsoft Office documents, PDF and text files on Google's servers to allow a user to run remote searches from multiple computers, but, according to the EFF, this presents a lucrative target to malicious hackers. Google said users can use a "Clear my Files" button to manually remove all files from its servers or a "Don't Search These Items" preference to remove specific files and folders from the software's index.
Source: http://security.ithub.com/article/EFF+Dont+Use+Google+Deskto p/171267_1.aspx

36. *February 10, IT Observer* — **DoJ announces national computer security survey.** The Department of Justice (DoJ) announced plans Friday, February 10, to conduct the first−ever national survey to measure the prevalence and impact of cybercrime on businesses within the

United States. The survey, conducted by DoJ's Bureau of Justice Statistics and the Department of Homeland Security's National Cyber Security Division, will estimate the number of cyber attacks, frauds and thefts of information and the resulting losses during 2005. The survey, which will start this month and will be completed by the end of the year, will provide critical information for businesses, industry, government and other users to make more informed decisions about how to target resources to fight cybercrime. The comprehensive survey will collect information from a wide range of industry sectors. Currently no national baseline measure exists on the extent of cybercrime. The survey data will enable the federal government to assess what needs to be done to reduce computer security vulnerabilities and will provide the first official national statistics on the extent and consequences of cybercrime among the country's 5.3 million firms with salaried employees..
Additional details about this survey: http://www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm
Source: http://www.ebcvg.com/press.php?id=2071

37. *February 10, Tech Web* — **DHS weathers Cyber Storm.** The U.S. Department of Homeland Security (DHS) still has to evaluate how well it fared through a series of simulated cyber attacks this week, but government and private companies avoided real−world damage and complications during their preparedness exercise. More than 100 public, private and international groups participated in mock attacks replicating the invasion of a utility company's computer system and the disruption of power grids. The exercise, called Cyber Storm, was designed to test the abilities of private companies and government agencies to deal with a major cyber security incident. DHS announced the completion of the exercise on Friday, February 10, but has yet to fully evaluate how effectively the groups communicated, cooperated and responded. Participants will evaluate the exercise, gauge interagency coordination and try to identify how current policies would affect response and recovery in the event of a real attack. The lessons learned this week are expected to be incorporated into a National Response Plan, which could be used if real attacks occur.
Source: http://www.techweb.com/wire/security/179103522;jsessionid=WOVM0LSQLDIUSQSNDBCSKHSCJUMEKJVN

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of multiple critical remote access vulnerabililities reported in versions 6.5.4 and 7.0 (and possibly earlier versions) of IBM Lotus Notes and IBM Lotus Domino iNotes Client.

US−CERT recommends users closely review the vulnerability reports. Solution to most of these vulnerabilities has been identified as upgrade to Version 6.5.5 of 7.0.1 of Lotus Notes.

US−CERT is aware of several vulnerabilities in Mozilla. Successful exploitation may

allow a remote, unauthenticated attacker to execute arbitrary JavaScript commands with elevated privileges or cause a denial of service condition on a vulnerable system.

For more information please review US−CERT Vulnerability Note: VU#592425 Mozilla based browsers fail to validate user input to the attribute name in "XULDocument.persist" at URL: http://www.kb.cert.org/vuls/id/592425

US−CERT urges users and administrators to implement the following recommendations. Review updates to:
Firefox 1.5.0.1: http://www.mozilla.com/firefox/
SeaMonkey 1.0: http://www.mozilla.org/projects/seamonkey/

Disable JavaScript in Thunderbird and Mozilla Suite.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 139 (netbios−ssn), 80 (www), 135 (epmap), 18551 (−−−), 54000 (−−−), 6999 (iatp−normalpri) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer